RECORD AND BRIEFS

No. 16-402

Supreme Court, U.S.
FILED
AUG 14 2017
OFFICE OF THE CLERK

In The

# Supreme Court of the United States

TIMOTHY IVORY CARPENTER,

*Petitioner,*

v.

UNITED STATES OF AMERICA,

*Respondent.*

**On Writ of Certiorari to the United States Court of Appeals for the Sixth Circuit**

## BRIEF OF *AMICUS CURIAE* RESTORE THE FOURTH, INC. IN SUPPORT OF PETITIONER

MAHESHA P. SUBBARAMAN
*Counsel of Record*
SUBBARAMAN PLLC
222 S. 9th St., Ste. 1600
Minneapolis, MN 55402
(612) 315-9210
mps@subblaw.com

August 14, 2017

COCKLE LEGAL BRIEFS (800) 225-6964
WWW.COCKLELEGALBRIEFS.COM

Library of Congress

TABLE OF CONTENTS

Page

Table of Authorities ..... ii

Interest of the *Amicus Curiae* ..... 1

Summary of the Argument ..... 2

Argument ..... 3

I. The Court's Fourth Amendment analysis of cell-site location information (CSLI) should recognize that privacy is relational ..... 3

II. The Court's Fourth Amendment analysis of CSLI should recognize that CSLI will become even more revealing over time ..... 9

III. The Court's Fourth Amendment analysis of CSLI should recognize that police use of CSLI comes with a high risk of abuse ..... 14

Conclusion ..... 18

# TABLE OF AUTHORITIES

Page

CASES

*Boyd v. United States*, 116 U.S. 616 (1886) ..... 3, 10, 18

*Brinegar v. United States*, 338 U.S. 160 (1949) ..... 15, 16

*Cohens v. Virginia*, 19 U.S. 264 (1821) ..... 9

*Commonwealth v. Augustine*, 4 N.E.3d 846 (Mass. 2014) ..... 10

*Ehling v. Monmouth-Ocean Hosp. Serv. Corp.*, 961 F. Supp. 659 (D.N.J. 2013) ..... 7

*Elonis v. United States*, 135 S. Ct. 2001 (2015) ..... 7

*Kyllo v. United States*, 533 U.S. 27 (2001) ..... 9, 10, 13

*Lane v. Facebook, Inc.*, 696 F.3d 811 (9th Cir. 2012) ..... 7, 8

*Miller v. United States*, 425 U.S. 435 (1976) ..... 4

*Olmstead v. United States*, 277 U.S. 438 (1928) ..... 2, 4, 5

*Ornelas v. United States*, 517 U.S. 690 (1996) ..... 3

*Riley v. California*, 134 S. Ct. 2473 (2014) ..... 19

*Smith v. Maryland*, 442 U.S. 735 (1979) ..... 4

*State v. Earls*, 70 A.3d 630 (N.J. 2013) ..... 11

*State v. Tate*, 849 N.W.2d 798 (Wis. 2014) ..... 9

*United States v. Carloss*, 818 F.3d 988 (10th Cir. 2016) ..... 6, 8

*United States v. Carpenter*, 819 F.3d 880 (6th Cir. 2016) ..... 10

TABLE OF AUTHORITIES – Continued

Page

*United States v. Jones*, 565 U.S. 400 (2012) .....8

*Weems v. United States*, 217 U.S. 349 (1910) .....9, 11

CONSTITUTIONAL PROVISION

U.S. Const., amend. IV .....*passim*

OTHER AUTHORITIES

AMNESTY INT'L, "IT'S ENOUGH FOR PEOPLE TO FEEL IT EXISTS": CIVIL SOCIETY, SECRECY, & SURVEILLANCE IN BELARUS (2016), http://bit.ly/2uuF7Fv .....16, 17

Andrea Peterson, *LOVEINT: When NSA Officers Use Their Spying Power on Love Interests*, WASH. POST, Aug. 24, 2013, http://wapo.st/15kehuK .....16

Brad Heath, *Police Secretly Track Cellphones to Solve Routine Crimes*, USA TODAY, Aug. 23, 2015, http://usat.ly/1JeqgNk .....15

Brian L. Owsley, *TriggerFish, StingRays, & Fourth Amendment Fishing Expeditions*, 66 HASTINGS L.J. 183 (2014) .....13

Charles Blain, *Police Could Get Your Location Data Without a Warrant. That Has to End*, WIRED, Feb. 2, 2017, http://bit.ly/2jGGRkA .....16

Frank Main, *Chicago Cops Lose Bid to Toss Lawsuit Over Secret Cell-Phone Tracking*, CHICAGO SUN-TIMES, Jan. 11, 2016, http://bit.ly/2uwZc9M .....17, 18

TABLE OF AUTHORITIES – Continued

Page

*If These Walls Could Talk: The Smart Home & the Fourth Amendment Limits of the Third Party Doctrine*, 130 HARV. L. REV. 1924 (2017) ..... 14

Jane Bambauer, *Other People's Papers*, 94 TEX. L. REV. 205 (2015) ..... 12

Jennifer Valentino-DeVries, *Police Snap Up Cheap Cellphone Trackers*, WALL ST. J., Aug. 19, 2015, http://on.wsj.com/2ux3Ep0 ..... 18

Jonathan Bard, *Unpacking the Dirtbox: Confronting Cell Phone Location Tracking with the Fourth Amendment*, 57 BOSTON COLLEGE L. REV. 731 (2016) ..... 13

Laurent Sacharoff, *The Relational Nature of Privacy*, 16 LEWIS & CLARK L. REV. 1249 (2012) ..... 4, 5

Mara H. Gottfried, *Minneapolis Officer Quits Amid Federal Probe of Metro Gang Strike Force*, PIONEER PRESS, Aug. 28, 2009, http://bit.ly/2vWk1is ..... 16

Michael Byrne, *New Indoor Positioning System Tracks Your Phone Using Sound Waves*, MOTHERBOARD, Apr. 2, 2016, http://bit.ly/2fEm5Wd ..... 12

Natasha H. Duarte, *The Home Out of Context: The Post-*Riley *Fourth Amendment & Law Enforcement Collection of Smart Meter Data*, 93 N.C. L. REV. 1140 (2015) ..... 14

Parmy Olson, *Algorithm Aims to Predict Crime by Tracking Mobile Phones*, FORBES, Aug. 6, 2012, http://bit.ly/2wzXDcO ..... 12

TABLE OF AUTHORITIES – Continued

Page

Robert H. Sloan & Richard Warner, *Relational Privacy: Surveillance, Common Knowledge, and Coordination*, 11 UNIV. OF ST. THOMAS J.L. & PUB. POL'Y 1 (2017).....6

Robert M. Bloom & William T. Clark, *Small Cells, Big Problems: The Increasing Precision of Cell Site Location Information & the Need for Fourth Amendment Protections*, 106 J. CRIM. LAW & CRIMINOLOGY 167 (2016).....11

Tom Simonite, *Bringing Cell-Phone Location-Sensing Indoors*, MIT TECH. REV., Aug. 31, 2010, http://bit.ly/2fEJcA9.....12

Tom Simonite, *This Phone App Knows If You're Depressed*, MIT TECH. REV., Sept. 22, 2014, http://bit.ly/2w35PoW.....12

WESLEY CHENG, CTR. FOR THE ADVANCEMENT OF PUBLIC INTEGRITY, COLUMBIA LAW SCHOOL, DOES SEEKING CELL SITE LOCATION INFORMATION REQUIRE A SEARCH WARRANT? (2016), http://bit.ly/2uuCOSB.....14

## INTEREST OF THE *AMICUS CURIAE*[1]

Restore the Fourth, Inc. is a national, non-partisan civil liberties organization dedicated to robust enforcement of the Fourth Amendment to the United States Constitution. Restore the Fourth believes that everyone is entitled to privacy in their persons, homes, papers, and effects and that modern changes in technology, governance, and law should foster the protection of this right.

To advance these principles, Restore the Fourth oversees a network of local chapters, whose members include lawyers, academics, advocates, and ordinary citizens. Each chapter devises a variety of grassroots activities designed to bolster political recognition of Fourth Amendment rights. On the national level, Restore the Fourth also files amicus briefs in significant Fourth Amendment cases.[2]

---

[1] This amicus brief is filed based on the blanket letters of consent that both Petitioner and Respondent have filed with the Court. No counsel for a party authored this brief in whole or in part; nor has any person or entity, other than Restore the Fourth, Inc. and its counsel, contributed money intended to fund the preparation or submission of this brief.

[2] *See, e.g.*, Brief of *Amicus Curiae* Restore the Fourth, Inc. in Support of Petitioners, *Hernandez v. Mesa*, 137 S. Ct. 2003 (2017) (No. 15-118); Brief of *Amicus Curiae* Restore the Fourth, Inc. in Support of Plaintiff-Appellee Araceli Rodriguez, *Rodriguez v. Swartz*, No. 15-16410 (9th Cir. filed May 7, 2016); Brief of *Amicus Curiae* Restore the Fourth, Inc. in Support of Defendant-Appellant Stavros Ganias, *United States v. Ganias*, 824 F.3d 199 (2d. Cir. 2016) (No. 12-240-cr) (en banc).

## SUMMARY OF THE ARGUMENT

Nearly 90 years ago, Justice Brandeis warned that the "progress of science in furnishing the Government with means of espionage [was] not likely to stop with wire-tapping." *Olmstead v. United States*, 277 U.S. 438, 474 (1928) (Brandeis, J., dissenting). Justice Brandeis also predicted "[w]ays may some day be developed" that would let the government pry into a person's "unexpressed beliefs, thoughts, and emotions." *Id.*

That day has arrived.

This case is about cell-site location information, or CSLI, which is generated when a person uses a cell phone. CSLI currently makes it possible for the police to know every place that a person has been and every social connection that a person has made over a period of time. CSLI also stands to make it possible for the police to predict a person's future location with a high degree of accuracy. Hence, with a person's CSLI in hand, the police now have the power to pry into that person's unexpressed beliefs, thoughts, and emotions.

Given this reality, any Fourth Amendment analysis of CSLI should be guided by the following three principles. First, privacy is relational in nature, which means that persons may have a reasonable expectation of privacy in their disclosures to third parties (e.g., a wireless service provider). Second, technological innovation will render CSLI even more revealing over time. Third, practical experience teaches that police use of CSLI comes with high risk of abuse.

## ARGUMENT

### I. The Court's Fourth Amendment analysis of cell-site location information (CSLI) should recognize that privacy is relational.

The Fourth Amendment to the United States Constitution states that "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized." This language "demonstrates a strong preference for searches [to be] conducted pursuant to a warrant." *Ornelas v. United States*, 517 U.S. 690, 699 (1996).

This preference cannot be enforced, however, without some explanation of the privacy interests that the Fourth Amendment is meant to protect. A definition of privacy is central to identifying whether a "search" has taken place and, if so, whether the warrant rule or an exception applies (e.g., exigent circumstances). This Court's early Fourth Amendment jurisprudence bears out this point. In *Boyd v. United States*, the Court emphasized that the Fourth Amendment is about more than "the breaking of . . . doors, and the rummaging of . . . drawers." 116 U.S. 616, 630 (1886). Rather, the Fourth Amendment is meant to address "all invasions on the part of the government and its employés of . . . the privacies of life." *Id.*

The Court's subsequent analysis of the privacies of life has led the Court to conclude that "a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties." *Smith v. Maryland*, 442 U.S. 735, 743–44 (1979). The Court has justified this conclusion on the ground that a person "takes the risk, in revealing his affairs to another, that the information will be conveyed by that person to the Government." *Miller v. United States*, 425 U.S. 435, 443 (1976). And the Court has found this conclusion holds true even when a person reveals information to a third party "on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed." *Id.*

This analysis reduces the Fourth Amendment's protection of the privacies of life to "an all-or-nothing concept," such that once "a person has waived or ceded privacy to one person she has ceded it to all."[3] But that is not how privacy works in the real world, nor is it consistent with the intent of the Framers in adopting the Fourth Amendment. Justice Brandeis recognized as much in his now-celebrated dissent in *Olmstead v. United States*, 277 U.S. 438 (1928). Rejecting the majority's conclusion that the Fourth Amendment did not apply to police wiretapping, Justice Brandeis explained that by adopting the Fourth Amendment, the Framers "conferred, **as against the**

---

[3] Laurent Sacharoff, *The Relational Nature of Privacy*, 16 LEWIS & CLARK L. REV. 1249, 1251 (2012).

**Government**, the right to be let alone." *Id.* at 478 (bold added).

Justice Brandeis thus made it clear that privacy is *relational* in nature, and the Fourth Amendment is concerned with shielding the privacies of life *from the government*. That purpose cannot be advanced by the conclusion that no reasonable expectation of privacy can reside in what we choose to disclose to third parties *who are not the government*. "[C]ommon sense tells us we treat privacy differently with different people and different classes of people. What we disclose to a spouse or partner we might not wish to disclose to the public or even a friend."[4] By the same token, our willingness to disclose information to a friend or a third-party service provider does not translate to a willingness to disclose the same information to the government—an entity that is "certainly different from friends and . . . private institutions—its criminal enforcement arm so much the greater."[5]

The relational nature of privacy is also apparent from the reality that "[w]hen we talk about privacy we must look at the manner and purpose of any intrusion."[6] "If a doctor looks in someone's wallet to find an emergency contact, that is far less an intrusion than if

---

[4] *Id.* at 1271.

[5] *Id.* at 1274.

[6] *Id.* at 1250.

a jealous spouse looks there for evidence of infidelity . . . .[7] Likewise, "a [police] officer approaching your home to return your lost dog or to solicit for charity may not be conducting a 'search' within the meaning of the Fourth Amendment. But one calling to investigate a crime surely is." *United States v. Carloss*, 818 F.3d 988, 1004 (10th Cir. 2016) (Gorsuch, J., dissenting).

Finally, the relational nature of privacy is apparent from the social limits that third parties observe when information is disclosed to them. These "specific patterns of informational restraint" depend on "the social roles in which people interact."[8] For example, pharmacists tend not to view the disclosure of prescription information to them as license to ask about their customers' personal lives.[9] It therefore makes no sense to conclude that individuals can never have any reasonable expectation of privacy in their disclosures to third parties. Depending on the social relationship involved, the exact opposite is often true: disclosures to a third party are often the result of people reasonably expecting that a third party will neither pry into the disclosure nor exploit it (i.e., as distinct from the mere expectation that a third party will not reveal the disclosure to others).

---

[7] *Id.*

[8] Robert H. Sloan & Richard Warner, *Relational Privacy: Surveillance, Common Knowledge, and Coordination*, 11 UNIV. OF ST. THOMAS J.L. & PUB. POL'Y 1, 7 (2017).

[9] *See id.*

The digital age, in turn, makes understanding privacy in relational terms all the more important. Consider the "social networking Web site Facebook." *Elonis v. United States*, 135 S. Ct. 2001, 2004 (2015). Facebook enables users to "post items . . . that are accessible to other users" and to the general public. *Id.* Facebook also "allows users to select privacy settings" that limit the public visibility of user posts. *Ehling v. Monmouth-Ocean Hosp. Serv. Corp.*, 961 F. Supp. 659, 668 (D.N.J. 2013). "Access can be limited to the user's Facebook friends, to particular groups or individuals, or to just the user." *Id.* This means that privacy on Facebook is not an all-or-nothing decision between global disclosure and total secrecy. Instead, privacy is a relational matter, with users choosing who gets to see their posts and who does not.

It is for this reason that a public revolt occurred in 2007 when Facebook adopted a new advertising program called Beacon. *See Lane v. Facebook, Inc.*, 696 F.3d 811, 816 (9th Cir. 2012). Through this program, the profiles of Facebook users began to display information about these users' activities on other websites—e.g., book purchases they made on a bookseller's website. *See id.* Facebook did not seek user consent for these disclosures. *See id.* As a result, many Facebook users "complained that Beacon was causing publication of otherwise private information about their outside web activities to their personal profiles without their knowledge or approval." *Id.* These complaints—and considerable public outcry—led Facebook to end Beacon and to pay $9.5 million to settle a class-action

lawsuit alleging Beacon violated various consumer privacy laws. *See id.* at 816–17.

While digital age developments like Facebook Beacon shed new light on the relational nature of privacy, they are not the only proof of this reality. Similar proof may be found in the "common-law trespassory test" for Fourth Amendment violations that this Court has revived in recent years. *United States v. Jones*, 565 U.S. 400, 414 (2012). The history behind this test teaches that the preservation of privacy through property rights is not an all-or-nothing proposition. One can license third parties to access one's private property while still retaining ultimate control over the property. *See Carloss*, 818 F.3d at 1006 (Gorsuch, J., dissenting) ("[T]he original meaning of the Fourth Amendment [and] centuries of common law recogniz[es] that homeowners may revoke by word or deed the licenses they themselves extend."). The quintessential example of this is a "no trespassing" sign, which lets property owners choose which third parties are welcome on their property (if any) and which ones are not. *See id.* at 1005 (explaining that homeowners may use no-trespassing signs to "mak[e] it clear to . . . 'solicitors, hawkers, and peddlers,' . . . that their presence on the curtilage is unwelcome").

With this in mind, the Court should commence its Fourth Amendment analysis of cell-site location information by "reconsider[ing] the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties." *Jones*, 565 U.S. at 417 (Sotomayor, J., concurring). The Fourth Amendment allows us to hold private *as*

*against the government* that which we share with others. And under this relational view of privacy, the Fourth Amendment status of CSLI may boil down to one simple fact: "People do not buy cell phones to have them serve as government tracking devices. They do not expect the government to track them by using [CSLI] . . . ." *State v. Tate*, 849 N.W.2d 798, 815 (Wis. 2014) (Abrahamson, C.J., dissenting).

## II. The Court's Fourth Amendment analysis of CSLI should recognize that CSLI will become even more revealing over time.

In applying the Fourth Amendment, this Court has long recognized that it must contemplate not only "what has been" but also "what may be." *Weems v. United States*, 217 U.S. 349, 374 (1910). For good reason. "Time works changes" and "brings into existence new conditions and purposes." *Id.* Forward-looking Fourth Amendment analysis subsequently ensures that "[r]ights declared in words" are not "lost in reality." *Id.*; *see also Cohens v. Virginia*, 19 U.S. 264, 387 (1821) (Marshall, C.J.) ("[A] constitution is framed for ages to come, and is designed to approach immortality as nearly as human institutions can approach it.").

Forward-looking Fourth Amendment analysis is especially critical where new technology is involved. *Kyllo v. United States*, 533 U.S. 27 (2001) cements this point. Confronted with the warrantless use of a thermal imager to view the inside of a home, this Court recognized that it could not confine its Fourth Amendment analysis to the "relatively crude" imager at issue.

*Id.* at 36. The Court also had to consider the "more sophisticated systems that are already in use or in development." *Id.* This led the Court to find that a Fourth Amendment violation had occurred. *See id.* The Court thereby refused to "leave the homeowner at the mercy of advancing technology . . . that could discern all human activity in the home." *Id.*

Similar forward-looking concern is required in any Fourth Amendment analysis of cell-site location information. In this case, the CSLI at issue consists of the call records that a wireless cellular provider logged and stored over a 127-day period for a single cell-phone subscriber (Mr. Carpenter). *See United States v. Carpenter*, 819 F.3d 880, 885–86 (6th Cir. 2016). The call records established the "date, time, and length of each call" that the subscriber made during the 127-day period. *Id.* The call records also established "the phone numbers engaged on [each] call" and "the cell sites where the call began and ended." *Id.* And with these call records in hand, the police were able to create maps showing that the subscriber's phone was located within 0.5 to 2 miles of certain robbery sites around when each robbery occurred. *Id.*

From this bare description of the CSLI at issue in this case, it is already possible to discern the remarkable capacity of CSLI to intrude on "the privacies of life." *Boyd*, 116 U.S. at 630. Indeed, CSLI constitutes "a treasure trove of very detailed and extensive information about [an] individual's 'comings and goings' in both public and private places." *Commonwealth v. Augustine*, 4 N.E.3d 846, 863 (Mass. 2014). And this treasure trove includes "not only where individuals are located at a point in time but also which shops,

doctors, religious services, and political events they go to, and [the persons] with whom they choose to associate." *State v. Earls*, 70 A.3d 630, 632 (N.J. 2013).

But this is only the beginning for CSLI. Contemplating "what may be" in regard to CSLI points to a future in which CSLI reveals even more about the privacies of life. *Weems*, 217 U.S. at 374. This is true for at least three reasons:

**First**, "[b]ecause of recent evolutions in cellular network technology, CSLI will soon paint an even more precise picture of a person's location history."[10] In particular, the growing "integration of small cell technologies into cellular networks" will enable CSLI to "reveal a cell phone user's location to within fewer than ten feet."[11] CSLI will consequently become even "more accurate than location data generated from GPS technologies, which can determine location to within only fifty feet."[12] And this innovation stands to become a reality sooner rather than later given that the Federal Communications Commission has "recently updated its rules on cellular networks to promote the installation of small cells."[13]

---

[10] Robert M. Bloom & William T. Clark, *Small Cells, Big Problems: The Increasing Precision of Cell Site Location Information & the Need for Fourth Amendment Protections*, 106 J. CRIM. LAW & CRIMINOLOGY 167, 170 (2016).

[11] *Id.* at 176.

[12] *Id.*

[13] *Id.* Another way CSLI stands to paint a more detailed portrait of a person's location history is through the advent of new

**Second**, the power and capacity of computers to extract meaning from CSLI grows with each passing day. Computing in general "facilitates aggregation, persistence, and searchability."[14] Applied to CSLI, sophisticated computing algorithms may soon make it possible for CSLI to reveal not only where a given person has been but also where that person is likely to be in the future. In fact, one researcher has already accomplished this feat on a small scale, "predicting the movements of 25 volunteers working in a town in Switzerland."[15] "He used GPS data, telephone numbers and their texting and calling history to do it, and the algorithm was at times able to predict where these volunteers were heading to within 20 square meters."[16]

**Third**, the number of devices enabling the police to obtain CSLI without going through a third-party wireless provider continues to grow. These devices go

---

technologies that make it easier for cell phones to establish a person's exact position while indoors. *See, e.g.*, Michael Byrne, *New Indoor Positioning System Tracks Your Phone Using Sound Waves*, MOTHERBOARD, Apr. 2, 2016, http://bit.ly/2fEm5Wd; Tom Simonite, *Bringing Cell-Phone Location-Sensing Indoors*, MIT TECH. REV., Aug. 31, 2010, http://bit.ly/2fEJcA9.

[14] Jane Bambauer, *Other People's Papers*, 94 TEX. L. REV. 205, 217 (2015).

[15] Parmy Olson, *Algorithm Aims to Predict Crime by Tracking Mobile Phones*, FORBES, Aug. 6, 2012, http://bit.ly/2wzXDcO.

[16] *Id.* Sophisticated algorithms also stand to make it possible for CSLI to be used "to peek inside a person's mind and gauge mental health." Tom Simonite, *This Phone App Knows If You're Depressed*, MIT TECH. REV., Sept. 22, 2014, http://bit.ly/2w35PoW ("Motion, audio, and location data harvested from a smartphone can be analyzed to accurately predict stress or depression.").

by many names, including TriggerFish, StingRay, Gossamer, Harpoon, and Hailstorm.[17] These devices fool "nearby cell phones into believing that the device is a cell tower so that the cell phone's information is then downloaded into the [device]."[18] This ultimately allows the police to use CSLI "to determine, with a reasonable degree of certainty, . . . where an individual is located while a cell call is being placed."[19] And these devices are becoming more powerful all the time, with one of the latest iterations being a plane-mounted "two-foot-square box" that enables CSLI to be captured "from tens of thousands of cell phones" at a time.[20]

Taken together, the above points establish that Fourth Amendment analysis of CSLI must account for the ever more revealing nature of CSLI over time. Much like the thermal imager at issue in *Kyllo*, warrantless use of CSLI stands to permanently "erode the privacy guaranteed by the Fourth Amendment." 533 U.S. at 34. The Court should not leave individuals at "the mercy of [this] advancing technology." *Id.* at 36. The stakes are too high. "CSLI is only the tip of the iceberg when it comes to personal data that is now

---

[17] *See* Brian L. Owsley, *TriggerFish, StingRays, & Fourth Amendment Fishing Expeditions*, 66 HASTINGS L.J. 183, 185 (2014).

[18] *Id.*

[19] *Id.* at 193.

[20] Jonathan Bard, *Unpacking the Dirtbox: Confronting Cell Phone Location Tracking with the Fourth Amendment*, 57 BOSTON COLLEGE L. REV. 731, 749–50 (2016).

routinely being collected by third parties."[21] The "relatively new Apple Watch," for example, "has the ability to track an individual much in the same way that smartphones can."[22] How the Court deals with CSLI will have a lasting influence on the privacy of information captured by many new technologies[23]—including those we cannot imagine yet.

## III. The Court's Fourth Amendment analysis of CSLI should recognize that police use of CSLI comes with a high risk of abuse.

Fourth Amendment analysis requires the Court to be forward-looking not only in how it thinks about technology but also in how it thinks about the police. The Court "must remember the authority which [it] concede[s] to conduct" warrantless searches "may be exercised by the most unfit and ruthless officers as well as by the fit and responsible, and resorted to in

---

[21] WESLEY CHENG, CTR. FOR THE ADVANCEMENT OF PUBLIC INTEGRITY, COLUMBIA LAW SCHOOL, DOES SEEKING CELL SITE LOCATION INFORMATION REQUIRE A SEARCH WARRANT? 4 (2016), http://bit.ly/2uuCOSB.

[22] *Id.*

[23] *See, e.g., If These Walls Could Talk: The Smart Home & the Fourth Amendment Limits of the Third Party Doctrine*, 130 HARV. L. REV. 1924, 1924 (2017) ("Smart home technologies necessitate the sharing of personal information across a multitude of third-party service providers . . . ."); Natasha H. Duarte, *The Home Out of Context: The Post-*Riley *Fourth Amendment & Law Enforcement Collection of Smart Meter Data*, 93 N.C. L. REV. 1140, 1141 (2015) ("[S]mart meters take information about the activities that occur inside the home and put it in the hands of a third party—the utility company.").

case of petty misdemeanors as well as in the case of the gravest felonies." *Brinegar v. United States*, 338 U.S. 160, 182 (1949) (Jackson, J., dissenting). The Court must also remember that to the extent it grants any kind of authority to search, the police will be the first interpreters of this authority and they will push this authority "to the limit." *Id.*

On this score, the instances in which cell-site location information has been abused by the police are too numerous to count. Chief among these abuses has been police concealment of CSLI use from both the public and the courts themselves. For example, "[i]n one case after another, *USA Today* found police in Baltimore and other cities used the phone tracker, commonly known as a stingray, to locate the perpetrators of routine street crimes and frequently concealed that fact from the suspects, their lawyers and even judges."[24] This abuse was systematic and rampant: the police "used stingrays to catch everyone from killers to petty thieves" and then "regularly hid or obscured that surveillance once suspects got to court," such that "many of those they arrested were never prosecuted."[25]

Another police abuse of CSLI that has come to light in recent years is CSLI-based surveillance of romantic interests. Take the case of a Minnesota woman who obtained "a restraining order against her boyfriend, a state narcotics agent who she claimed abused

---

[24] Brad Heath, *Police Secretly Track Cellphones to Solve Routine Crimes*, USA TODAY, Aug. 23, 2015, http://usat.ly/ 1JeqgNk.

[25] *Id.*

his access to cell-site data information to stalk her."[26] "She was granted the [restraining] order and the man is no longer a police officer."[27]

Of course, this kind of abuse is not confined to CSLI. As the *Washington Post* has found, "[t]here are plenty of cases in which local law enforcement officials have been accused of abusing their access to [police] databases to acquire information about potential romantic interests."[28] But this reality only underscores the extent to which police use of CSLI, free from Fourth Amendment restraints, increases the risk of abusive CSLI-based surveillance of romantic interests.

Finally, there are those CSLI abuses that have taken place abroad, demonstrating how CSLI can be used to "cow[] a population, crush[] the spirit of the individual and put[] terror in every heart." *Brinegar*, 338 U.S. at 180 (Jackson, J., dissenting). Amnesty International has compiled a devastating report on such abuses in the former Soviet state of Belarus.[29] Under

---

[26] Charles Blain, *Police Could Get Your Location Data Without a Warrant. That Has to End*, WIRED, Feb. 2, 2017, http://bit.ly/2jGGRkA.

[27] *Id.*; *see also* Mara H. Gottfried, *Minneapolis Officer Quits Amid Federal Probe of Metro Gang Strike Force*, PIONEER PRESS, Aug. 28, 2009, http://bit.ly/2vWk1is.

[28] Andrea Peterson, *LOVEINT: When NSA Officers Use Their Spying Power on Love Interests*, WASH. POST, Aug. 24, 2013, http://wapo.st/15kehuK.

[29] AMNESTY INT'L, "IT'S ENOUGH FOR PEOPLE TO FEEL IT EXISTS": CIVIL SOCIETY, SECRECY, & SURVEILLANCE IN BELARUS 6–8 (2016), http://bit.ly/2uuF7Fv.

Belarusian law, "mobile telephone [and] internet providers . . . are required to allow the authorities direct access to their customers' data."[30] This places Belarusians in constant fear of being tracked by the police through CSLI. For a Belarusian journalist, this has meant the frequent experience of "traveling to a town to meet activists with whom she had spoken on the phone, only to find that the police were waiting upon her arrival."[31] For a Belarusian human rights lawyer, this has meant being forced to suspect a "vehicle decked with antennae near protest events" was in fact "tracking protestors' phones."[32]

Troubling echoes of these fears also exist here at home. A freedom-of-information lawsuit against the Chicago Police Department has led to the production of public records establishing that Chicago has "spent more than $340,000 between 2005 and 2010 on cell-site simulators, as well as software upgrades and training."[33] "[The] fear is that police have been using the[se] devices to monitor protesters at events such as the NATO Summit. Demonstrators were suspicious that the batteries in their cellphones seemed to become

---

[30] *Id.* at 6.

[31] *Id.* at 21.

[32] *Id.*

[33] Frank Main, *Chicago Cops Lose Bid to Toss Lawsuit Over Secret Cell-Phone Tracking*, CHICAGO SUN-TIMES, Jan. 11, 2016, http://bit.ly/2uwZc9M.

quickly depleted during . . . protests—something caused by cell-tower simulators."[34]

Against this backdrop, with more and more police departments buying CSLI technology, the need to ensure this power is not abused has never been greater.[35] Any Fourth Amendment analysis of CSLI must account for this need. "It is the duty of courts to be watchful for the constitutional rights of the citizen, and against any stealthy encroachments thereon." *Boyd*, 116 U.S. at 635. That includes stealthy police use (and abuse) of CSLI.

## CONCLUSION

Given the relational nature of privacy, the increasingly revealing nature of cell-site location information, and the high risk of CSLI abuse, the Court should hold that the Fourth Amendment governs CSLI. The Court should then find that "the question of what police must

---

[34] *Id.*

[35] *See* Jennifer Valentino-DeVries, *Police Snap Up Cheap Cellphone Trackers*, WALL ST. J., Aug. 19, 2015, http://on.wsj.com/2ux3Ep0.

do before searching [CSLI] . . . is accordingly simple—get a warrant." *Riley v. California*, 134 S. Ct. 2473, 2495 (2014).

Respectfully submitted,

MAHESHA P. SUBBARAMAN
*Counsel of Record*
SUBBARAMAN PLLC
222 S. 9th St., Ste. 1600
Minneapolis, MN 55402
(612) 315-9210
mps@subblaw.com

*Counsel for Amicus Curiae Restore the Fourth, Inc.*

Dated: August 14, 2017